ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

November 7, 2000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF THE DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS AND SERVICES
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS, JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES

SUBJECT: Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information Systems

Mobile code[1] is a powerful software tool that enhances cross-platform capabilities, sharing of resources, and web-based solutions. Its use is widespread and increasing in both commercial and government applications. In DoD, mobile code is employed in systems supporting functional areas ranging from acquisition to intelligence to transportation. Mobile code, unfortunately, has the potential to severely degrade DoD operations if improperly used or controlled.

[1] Mobile code is software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.

To protect DoD systems from the threat of malicious or improper use of mobile code, we must assess and control the risks imposed by the technology. The guidance in Enclosure 1 is the first step in an iterative process to reduce such risks to DoD information systems. It categorizes mobile code technologies and restricts their application within DoD based on their potential to cause damage if used maliciously. It is applicable to all DoD information systems used to process, transmit, store, or display DoD information, including commercial off-the-shelf (COTS) products and electronic commerce applications used but not owned by the government. Excepted are Special Access Program and Sensitive Compartmented Information systems and networks, laboratory or test-bed networks which cannot communicate directly with other networks, and application software components where the installation, network transferal and execution of the application is conducted totally within a single security enclave.

Testing of the controls imposed by Enclosure 1 to date has revealed minimal negative effects on DoD information systems, functions, and operations. However, additional in-depth operational testing will be conducted before this memorandum transitions to a formal DoD directive to ensure that no unintended consequences preclude conduct of any of the Department's legitimate functions, to include administrative, as well as mission critical and mission support activities. The test results will be distributed as they become available.

During the transition period, all DoD Components are directed to follow the policy guidance at Enclosure 1 as closely as possible. In those instances where the policy cannot be followed because of unacceptable documented consequences to mission, the Component Head (including OSD Principal Staff Assistants) responsible for the system or application in question shall ensure that the DoD CIO is informed of the use of the non-conforming mobile code, along with an assessment of associated risk and any known mitigation measures. The DoD CIO will in turn ensure that this information is provided to all affected DoD Components.

Definitions of terms used in this memorandum and associated material are at Enclosure 2. My point of contact for this policy guidance is Mr. Donald L. Jones in the Office of the Director for Infrastructure and Information Assurance at (703) 614-6640 or e-mail donald.l.jones@osd.pentagon.mil. For technical questions contact Lt Col Danny A. Flowers, Joint Staff Command, Control, Communications, and Computer (C4) Systems Directorate (J-6), Information Assurance Division (J6K) at commercial (703) 693-4578 or DSN 223-4578, e-mail danny.flowers@js.pentagon.mil.

Arthur L. Money

Attachments

Enclosure 1
Mobile Code Technology Risk Categories and Use Restrictions

1. The following paragraphs categorize and define mobile code technologies used within DoD based on risk, and restrict their application based on their potential to cause damage if used maliciously. Initial risk category assignments for commonly used mobile code technologies are listed in Attachment 1. Configuration guidance will be provided separately.

1.1. Category 1.

1.1.1. Category 1 mobile code technologies exhibit a broad functionality, allowing unmediated access to workstation, host and remote system services and resources. Category 1 mobile code technologies have known security vulnerabilities with few or no countermeasures once they begin executing. Execution of Category 1 mobile code typically requires an all or none decision, either execute with full access to all system resources or don't execute at all.

1.1.2. Category 1 mobile code technologies can pose a severe threat to DoD operations. However, the implementations of some mobile code technologies differentiate between *signed* and *unsigned* mobile code. These implementations can be configured to allow the execution of *signed* mobile code while simultaneously blocking the execution of *unsigned* mobile code. When Category 1 mobile code is *signed* and obtained from a trusted source, the risk is reduced.

1.1.3. Category 1 mobile code may be used in DoD information systems only when the mobile code is *signed* with a DoD-approved PKI code signing certificate and the mobile code is obtained from a trusted source. Until a DoD-approved PKI code-signing certificate is available, the responsible CIO may approve alternate commercially available code signing certificates.

1.1.4. To the extent possible, all DoD computer systems (e.g., hosts), workstations, and applications capable of executing mobile code shall be configured to disable the execution of *unsigned* Category 1 mobile code obtained from outside the enclave boundary. In situations where the use of *unsigned* Category 1 mobile code is critical to the performance of a mission, a written waiver for its use may be approved by the responsible CIO. The waiver should stipulate use of a mobile code security product, along with a security configuration for the product, to mitigate the risk posed by the *unsigned* category 1 mobile code. Until such time as mobile code security products validated by the National Information Assurance Partnership (NIAP) as specified in National Security Telecommunications and information Systems Security Policy (NSTISSP) Number 11 are available, the responsible CIO may approve the use of specific commercial-off-the-shelf (COTS) third party mobile code security products when granting a waiver for *unsigned* Category 1 mobile code use. The waiver shall be attached to the accreditation package as part of the System Security Authorization Agreement (SSAA) required by DoDI 5200.40.

1.1.5. All program offices with new procurement and development efforts that rely on Category 1 mobile code technologies (*signed* or *unsigned* w/waiver) shall include a mobile code risk mitigation strategy detailing the measures incorporated into the system development to curtail the risk posed by its use as part of their risk management plan, in accordance with DoDI 5200.40. The risk mitigation strategy shall be included in the accreditation package as part of the SSAA. No new DoD program may expend funds on the development or procurement of products or services that contain, use, or depend on the download and execution of Category 1 mobile code across enclave boundaries, unless that product or service uses *signed* mobile code as stipulated in paragraph 1.1.3. above.

1.2. Category 2

1.2.1. Category 2 mobile code technologies have full functionality, allowing mediated or controlled access to workstation, host, and remote system services and resources. Category 2 mobile code technologies may have known security vulnerabilities but also have known fine-grained, periodic, or continuous countermeasures or safeguards.

1.2.2. Category 2 mobile code technologies can pose a moderate threat to DoD information systems. The use of Category 2 mobile code technologies, when combined with prudent countermeasures against malicious use, can afford benefits that outweigh their risks.

1.2.3. Category 2 mobile code may be used in DoD information systems if the mobile code is obtained from a trusted source over an assured channel. In addition, *unsigned* Category 2 mobile code, whether or not obtained from a trusted source over an assured channel, may be used if it executes in a constrained environment without access to local system and network resources (e.g., file system, Windows registry, network connections other than to its originating host).

1.2.4. Where possible, web browsers and other mobile code enabled products shall be configured to prompt the user prior to the execution of Category 2 mobile code. Where feasible, protections against malicious Category 2 mobile code technologies shall be employed at end user systems and at enclave boundaries. The responsible CIO may grant a waiver for the use of Category 2 mobile code not obtained from a trusted source over an assured channel. If code signing is used to meet the requirement for a trusted source over an assured channel, a DoD-approved PKI code-signing certificate shall be used, if available. In the absence of a DoD-approved PKI code-signing certificate, the responsible CIO may approve alternate commercially available code signing certificates.

1.2.5. New procurement and development efforts that rely on Category 2 mobile code technologies shall include a mobile code risk mitigation strategy detailing the measures incorporated into the system development to curtail the risk posed by their use in their risk management plan, in accordance with DoDI 5200.40. The risk mitigation strategy shall be attached to the accreditation package as part of the SSAA. The responsible CIO must approve new procurement and development efforts that use Category 2 mobile code that does not meet the above restrictions (e.g., unsigned mobile code that does not execute in a constrained environment as described in paragraph 1.2.3. above, or mobile code not obtained from a trusted source over an assured channel).

1.3. Category 3

1.3.1. Category 3 mobile code technologies support limited functionality, with no capability for unmediated access to workstation, host, and remote system services and resources. Category 3 mobile code technologies may have a history of known vulnerabilities, but also support fine-grained, periodic, or continuous security safeguards.

1.3.2. Category 3 mobile code technologies pose limited risk to DoD systems. When combined with vigilance comparable to that required to keep any software system configured to resist known exploits, the use of Category 3 mobile code affords benefits that outweigh the risks.

1.3.3. Category 3 mobile code technologies may be used in DoD information systems.

1.3.4. Program Executive Officers (PEOs), Program Managers (PMs), and Executive Agents (EAs) shall develop a mobile code risk mitigation strategy as part of the risk management plan, in accordance with DoDI 5200.40. The risk mitigation strategy shall be attached to the accreditation package as part of the SSAA.

1.4. Emerging Mobile Code Technologies.

1.4.1. Emerging mobile code technologies refer to all mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet been reviewed for categorization.

1.4.2. Unless a waiver is granted under 1.4.3. below, the download and execution of mobile code using unwaivered emerging technologies shall be blocked by all means available at the enclave boundary, workstation, host, and within applications.

1.4.3. If an emerging mobile code technology is planned for use in a DoD application, the sponsoring Component will provide the DoD CIO sufficient information to evaluate and categorize the technology at least 90 days prior to initial use. If the emerging technology is not categorized within the 90-day period, the responsible CIO may grant a written waiver for its use.

1.4.4. Working through DISA, DoD will invite industry to provide a beta version of any new technology at least 90 days ahead of public release to give DoD an opportunity to evaluate and categorize it. Developers are encouraged to assist Component CIOs' efforts to sponsor categorization of emerging technologies.

2. Use of Mobile Code in E-mail.

2.1 Whenever possible, the automatic execution of all categories of mobile code in e-mail bodies and attachments shall be disabled.

2.2 Whenever possible, desktop software shall be configured to prompt the user prior to opening e-mail attachments that may contain mobile code.

Attachment

Attachment 1 to Enclosure 1
Initial Mobile Code Technology Risk Category Assignments

1. The mobile code technologies listed in paragraph 2 below are within the scope of the policy when employed in a manner satisfying the definition of mobile code found in Enclosure 2. For information and clarification, several data representation formats and technology application areas that are currently outside the scope of the policy are also identified in paragraph 3.

2. Category Assignments:

2.1.1. The following technologies are designated Category 1:

ActiveX
Windows Scripting Host, when used to execute mobile code
Unix Shell Scripts, when used as mobile code
DOS Batch Scripts, when used as mobile code

2.2.1. The following technologies are designated Category 2:

Java applets and other Java mobile code
Visual Basic for Applications (VBA)
LotusScript
PerfectScript
Postscript

2.31. The following technologies are designated Category 3:

Javascript (include Jscript and ECMAScript variants)
VBScript
Portable Document Format (PDF)
Shockwave/Flash

3. Exclusions:

3.1. Technology Exclusions. The following technologies are not presently designated as mobile code:

XML
SMIL
Quicktime
VRML (exclusive of any associated Java applets or JavaScript scripts. Applets or scripts associated with VRML worlds are subject to the policy).

3.2. Application Exclusions. The following technology application areas are outside the scope of the DoD mobile code policy.

3.2.1. Scripts and applets embedded in or linked to web pages and executed in the context of the web server. Examples of technologies in this application area include: Java servlets, Java Server Pages, CGI, Active Server Pages, CFML, PHP, SSI, server-side JavaScript, server-side LotusScript.

3.2.2. Local programs and command scripts. Examples of technologies in this application area include: binary executables, shell scripts, batch scripts, Windows Scripting Host (WSH), Perl scripts.

3.2.3. Distributed object-oriented programming systems – Examples of technologies in this area include: CORBA, DCOM. [Note: Java RMI and Java Jini technologies are included under section 3.2.1]

3.2.4. Software patches, updates, including self-extracting updates – software updates that must be invoked explicitly by the user are outside the scope of the mobile code policy. Examples of technologies in this area include: Netscape SmartUpdate, Microsoft Windows Update, Netscape web browser plug-ins, and Linux

Enclosure 2
Definitions

3.1. Assured Channel: A network communication link that is protected by a security protocol providing authentication and data integrity, and employs US Government approved cryptographic technologies whenever cryptographic means are utilized. The following protocols and mechanisms are sufficient to meet the requirements of authentication and data integrity protection for an assured channel: the Secret Internet Protocol Router Network (SIPRNET), Internet Protocol Security (IPSec), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Multipurpose Internet Mail Extension (S/MIME), or digital code signing using a DoD-approved PKI code signing certificate, and other systems using NSA-approved high assurance guards with link encryption methodology.

3.2. Code Signing Certificate: A public key infrastructure (PKI) certificate that can be used to digitally sign code. Such a certificate has a specially assigned attribute (referred to as the *code signing bit*) set.

3.3. Component Heads: For purposes of this policy guidance, the Component Heads include: the Office of the Secretary of Defense Principal Staff Assistants; the Secretaries of the Military Departments; the Chairman of the Joint Chiefs of Staff, the Commanders of the Combatant Commands, the Directors of the Defense Agencies; and, the Inspector General of the Department of Defense.

3.4. Enclave: For the purpose of this policy, an enclave is an information system environment that is end-to-end under the control of a single authority and has a uniform security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization (e.g., base, post, camp, or station) or a mission (e.g., Global Command and Control System (GCCS)) and may also contain multiple networks. As a standard, the enclave typically starts and ends at the premise router. For the purposes of this policy, Component domains with assured security boundaries can be treated as a single enclave

3.5. Malicious Mobile Code: Mobile code software modules designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, providing the unauthorized disclosure of information, corrupting information, denying service, or stealing resources.

3.6. Mediated Access: Access to system resources subject to the control and approval of a runtime-enforced security policy, either during execution or at the beginning of execution. A runtime-enforced security policy provides controlled access to system resources via an intermediary such as an interpreter, virtual machine, or a security manager.

3.7. Mobile Code: Mobile code is technology which allows for the creation of executable information which can be delivered to an information system and directly executed on any hardware/software architecture which has an appropriate host execution environment. This policy is focused on the receipt of executable information from sources outside the Designated Approving Authority's area of responsibility. Therefore, for the purposes of this policy, mobile code is software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.

3.8. Mobile Code Technologies: Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, VBScript, and ActiveX).

3.9. Trusted Source: A source that is adjudged to provide reliable software code or information and whose identity can be verified by authentication. The following mechanisms are sufficient to validate the identity of a trusted source: connection via the SIPRNET, digital signature over the mobile code itself using a DoD-approved PKI code signing certificate, a commercial code signing certificate approved by the DoD CIO, or authentication of the source of the transfer by public key certificate (e.g., S/MIME, SSL server certificate from an SSL web server).

3.10. Unmediated Access: Direct use of system resources, not subject to any approval or control beyond that imposed on conventional user applications.